Transactions of the Korean Nuclear Society Fall Meeting
Goyang, Korea, October 23-25, 2019

Electronic Information Management for New Build Nuclear Power Plants

Prof. Robert M. Field*, Prof. C. K. Chang†
Department of Nuclear Engineering, KEPCO International Nuclear Graduate School
**Corresponding Author* rmfield@kings.ac.kr , †ckchang@kings.ac.kr

1. Introduction

The rapid adoption and growth of Cloud storage is a good measure of widespread acceptance by the corporate world. With all of its attendant advantages, this phenomenon and its potential re-emphasizes the need for adequate planning to achieve effective configuration management for any new build Nuclear Power Plant (NPP) project. Comprehensive retention and access to all Data, Information, and Records (DIRs) for the life cycle of the plant is a key to maintaining: (i) effective and efficient adherence to (and revisions to) the design basis, (ii) timely and accurate reporting to government authorities, and (iii) safe and informed response to occurrences and discoveries during various phases of the project. Traditionally, electronic storage was not considered to be appropriate for NPP data retention (rather paper, microfilm, or microfiche was required). However, modern approaches to electronic storage are now considered to be 'permanent' as recently outlined by the National Archives of the USA government [1].

With this, we can propose an approach to structuring electronic data storage under the following topics: (i) DIR exchange paths, (ii) life cycle considerations, (iii) design criteria and data flow, and (iv) best practices. Such an approach is believed to provide a robust, secure, and economic approach to electronic data management for the life of a new build NPP.

2. Background

Nearly ten years ago the IAEA addressed application of modern day information technology for NPP configuration management [2]. Historically, DIRs required for the safe and reliable operation of NPPs were not always available. As stated by the IAEA, "*...the development of configuration management and the development of the mechanism for retention of design information were haphazard and inconsistent,*" and "*... this has presented a continuing challenge to the organizations responsible for safe and dependable plant operation.*"

As a consequence of inadequate collection and management of the design basis, in the 1990s, several nuclear units in the USA were shut down for many months and in some cases for years to bring documentation of the design basis back into compliance with the licensing basis (i.e., as provided to the regulatory authorities) (e.g., Dresden 2/3, LaSalle 1/2, Cook 1/2).

The capabilities of modern day electronic data storage allow for an integrated approach to DIR management. A single framework can be developed to store not only configuration management information, but also <u>ALL</u> data associated with the project (e.g., commercial, correspondence, design information, inspection and test records, personnel records, etc.). Key elements of the approach to DIR management are discussed below along with what are considered to be best practices to effectively and efficiently implement the program.

3. Modern Technology and DIR Exchange

Technology offered by modern Cloud service providers opens up a significant potential to improve DIR storage and access in the areas of security, ease of use, flexibility, and cost reduction. It is recognized that for any megaproject such as a new build NPP there will be great volume of DIRs exchanged among the various organizations which are involved. A simplified diagram of major DIR exchanges typical of the construction stage of such a project is provided in Fig. 1 below.

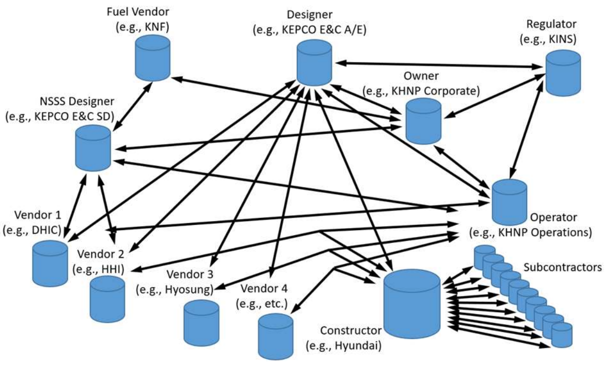

Fig. 1. Traditional DIR Flow for New Build NPP

With full utilization of Cloud storage and computing, this DIR flow can be untangled and automated. A simplified diagram of the proposed data flow is provided in Fig. 2 below.

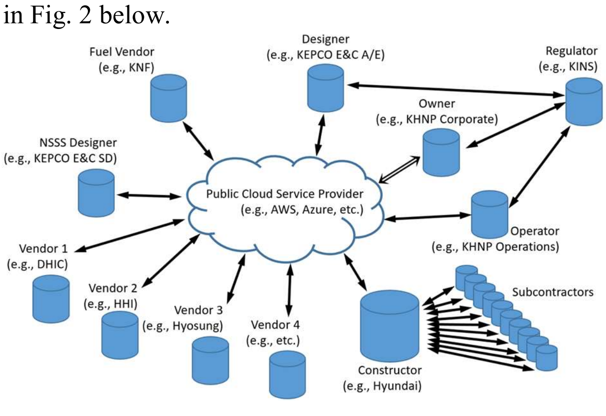

Fig. 2. Proposed DIR Flow for New Build NPP

Note that the Regulator is excluded from Cloud access so that the Owner can have absolute control over that communication channel.

Even with modern use of electronic data exchange of DIRs, by retaining the traditional communication approach (Fig. 1), significant overhead is required simply to: (i) communicate with various vendors, (ii) track deliverables, (iii) update project schedules, and (iv) process payments. With the proper design of a Data Management System (DMS), essentially all of these activities can be automated.

Further, the current offerings and capabilities of commercial Cloud services can greatly simplify this data flow with improved physical and cyber security at lower cost. This contention is a subject for a separate paper, but is taken as a given for the balance of the treatment here.

4. Life Cycle Considerations

The phases in the life cycle of an NPP are outlined by the IAEA [3] as follows:

1. Pre-project
2. Project Decision Making
3. Plant Construction
4. Plant Operation
5. Plant Decommissioning

These phases provide a good delineation for understanding the types of DIRs to be produced:

Pre-project – Information during this phase generally consists of analysis documents and reports including planning for: (i) the power system, (ii) legal and organizational framework, (iii) infrastructure, (iv) site survey and environmental assessment, and (v) manpower survey. This information is generally useful for historical context and for follow-on projects, but is not critical to operation of the new build NPP.

Project Decision Making – Documents in this phase include financing and site selection studies, but also include the first project specific documents, primarily related to initial bidding (i.e., specification, offers, and evaluation). This is followed by contract negotiation and signing. Secure retention of documents related to the bidding process in addition to corresponding procurement process documents for long lead items is required at this stage.

Plant Construction – This category includes development of most of the documentation related to the plant configuration, including: (i) design engineering and licensing, (ii) procurement, including vendor documentation (inspections, tests, drawings, and manuals), (iii) construction documents (welding records, inspections, testing, etc.), and (iv) commissioning.

Plant Operation – During plant operation, several types of documents are of interest and recommended for permanent storage. These include: (i) personnel records, (ii) inspection and test records, (iii) regulatory and environmental compliance records, (iv) training materials and test records (e.g., SRO training and testing), (v) fitness for duty records, (vi) maintenance records, (vii) plant procedures, (viii) modification packages, etc.

Decommissioning – Based on the time window for decommissioning, planning for this stage can be deferred.

From the above listing, it is clear that there is a wide range of the types and importance of the DIRs which are generated in the life of the plant. However, due to the modern day economy of long-term electronic storage, it is recommended here that ALL DIRs be retained with no consideration of a retention period. A rough estimate of the volume of data storage is as follows:

Table 1. Estimate of DIR Storage Volume

Description	No. (10^3)	Pages[1]	Storage
Design	200	100	2000 GB
Procurement	200	50	1000 GB
Licensing	10	100	100 GB
Construction	500	3	150 GB
Operation	0.2[2]	10	43,800 GB
Etc.	-	-	Small

1) Per DIR.
2) Daily output over 60 year operating lifetime.

From this estimate, it is expected that all non-operating stage records could be stored within an electronic storage volume of a few terabytes (10^{12} bytes). This is a very small amount of data relative to modern storage technology measured in petabytes (10^{15}) for major corporations and exabytes (10^{18}) for large government organizations. If the guesstimate for DIR storage volume during the operation stage is reasonable, special provisions may be required in the system framework to economically store this type of data. Note that online access to such data (particularly older records) is not required. *Also note that this estimate does not include big data volumes such as generated by thousands of channels of telemetry from operating equipment (particularly rotating equipment). Due to the volume and low sensitivity of this data, it is recommended that this data receive separate treatment from the approach here.*

5. Criteria and Data Flow

DIR generation in the various phases in the NPP life cycle listed above differs greatly with respect to the number of organizations which are submitting and retrieving documents from the database. Specifically, with the exception of Phase 3 – Construction, the number of interfacing organizations is very limited, with more that 90% of DIR uploads and retrievals expected from just a single organization (i.e., the Owner for Phases 1 and 2, and the plant operator for Phase 4), with Phase 5 not critical to the DIR framework and criteria. Since Phase 3 will see the greatest traffic in DIRs and the largest number of interfacing organizations, the focus here will be on this phase, with other phases generally covered by the Phase 3 activities.

5.1 Criteria

Full development of a framework for DIR storage and retrieval requires programmatic development of a detailed Design Criteria Manual (DCM). Such development is not possible in the space of this examination, but key, high level criteria to be considered are listed below.

1) Formal Documentation – The Data Management Plan (DMP) and system framework shall be formally maintained in a 'living' document which identifies the design criteria and other key items. A controlled Design Criteria Manual (DCM) shall also be prepared as a subsidiary to the plan.
2) Ease of Use – A single user interface to upload and retrieve documents shall be developed and used by all organizations with access to the DIR database. Storage shall be indexed to an extent which permits searchable queries further allowing simultaneous downloads of multiple associated documents.
3) Access – A single access matrix which links authorized individuals for specific document types and document vaults shall be maintained by the Owner. Only the Owner and Cloud service provider shall have access to the matrix.
4) Access Protocol – An access protocol, consisting of the levels of security applied to access (e.g., USERid, password, text verification, biometrics, embedded hardware keys, etc.) shall be assigned to each document type with levels of security appropriate to the type of DIR (e.g., low security for newsletters, highest security for safeguards information and personnel records).
5) DIR Organization – Data 'vaults' and 'sub-vaults' shall be created and each DIR shall be assigned to one and only one such location. Vaults shall have distinct access and authorization requirements. Access to vaults/sub-vaults shall be prudently restricted without the introduction of excessive barriers to ease of use for individuals with a demonstrated need for access.
6) Probing and Testing – Before rollout, the system framework shall be formally reviewed by internal and external audit teams to ensure compatibility with both security and compliance requirements.
7) Training – A formal training program in use of the DIR database shall be prepared and all individuals with access shall complete the training and pass a test prior to being granted access.
8) Operation – Each DIR in the database is uploaded once and only once. Upon confirmation of access credentials, the service provider shall affix to each uploaded DIR a metadata file which includes as a minimum: (i) genesis blockchain record, (ii) necessary project data (e.g., equipment number, OBS, PBS, WBS, FBS, schedule line item, etc.), and (iii) date, time, and other information as determined by the project team. The service provider shall then store the DIR in the appropriate vault/sub-vault and electronically notify the Owner of receipt permitting an automated update to the project schedule (and payment schedule if warranted).
9) Disaster Recovery and Offline Backup – The DMP shall include provisions for disaster recovery and for long-term offline, archival storage in a secured location (potentially non-encrypted).
10) Security 1 – DIRs shall have an assigned security class which is cross-linked to both access controls and to monitoring of queries.
11) Security 2 – DIRs shall receive robust encryption based on security class, with potentially two levels assigned (one at the user level, and a second one by the service provider).
12) Audit and Oversight – Formal audits shall be periodically conducted by qualified teams and individuals. The audits shall follow a formal plan and be documented in a formal report. The Owner shall form a permanent IT committee which authorizes contracts and budgets and performs oversight of the DMS including a formal review and formal acceptance of audit results.

5.2 Data Flow - Simplified Description

Proposed process steps (which meet the high level criteria listed above) for the upload and retrieval of a DIRs at the Cloud service provider are illustrated in Fig.'s 3 and 4 below.

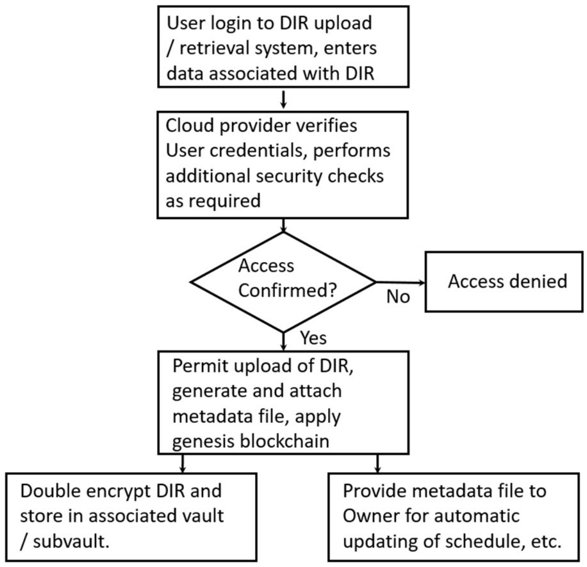

Fig. 3. DIR Upload Protocol

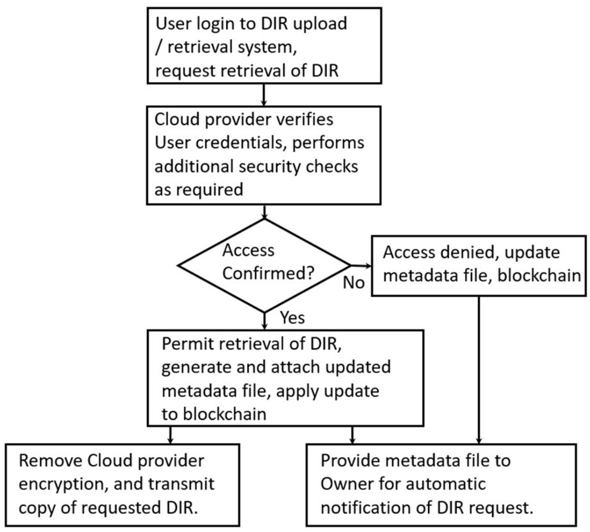

Fig. 4. DIR Retrieval Protocol.

6. Best Practices and Future Application

6.1 User Productivity

Productivity is a key element in the design of the interface between users and the database. Initial and periodic testing and refinement of the Graphical User Interface (GUI) with accounting of human factors is considered to be a best practice.

6.2 Security

Security is a cornerstone issue, but must not be considered as static. Best practices in this area include:

1. Initial review of the DMP by internal and external experts in security issues.
2. Adequate monitoring tools to detect internal and external intrusions.
3. Procedures for timely response to attempted or successful instructions.
4. Periodic whitehat exercises of intrusion detection and mitigation procedures.
5. Specific audit metrics related to security.

6.3 Operating Cost, Change of Vendor

Procurement contracts for Cloud services should ensure interoperability of data management between providers (both private and public) and for the orderly transfer of service to an alternative provider if that becomes warranted.

6.4 Training and communication

Users should be regularly updated on system changes, issues, and incidents through clear and open communication. Users should regularly be required to complete updated training.

6.5 Integration

The DIRs which are stored in the database represent more than simply an archive. Data should be catalogued in such a way that users can take maximum advantage of the electronic nature of the data. For example, users should be able to get comprehensive search results for DIRs across a broad domain of considerations. Examples include:

- Component outline drawings of a certain type and classification (e.g., ASME III, Class 2 titling disk check valves)
- All DIRs associated with plant equipment by component and part number
- Listing of DIRs which provides qualified welders by service dates and qualifications
- Listing of surveillance test records for a certain type of test

6.6 Metadata

The metadata file associated with each DIR should follow industry standard protocol such as the DCMES.

6.7 Living Data Management

The program should be a living program, adequately resourced to identify and implement improvements in the areas of usability, security, and cost reduction. A formal program to solicit, record, and respond to user input should be implemented. Such a program would record input in the area of errors, lessons learned, threats, and opportunities.

6.8 AI and Machine Learning

Use of a public Cloud service provider opens opportunities for efficient use of powerful tools in the areas of artificial intelligence and machine learning, with the ability to leverage vendor experts. Two examples of the many areas this technology may prove useful in the future are:

1. Weld X-ray Images – Historically, falsification of x-rays for safety related welds has been an industry issue, where one x-ray may be substituted for multiple welds. Use of image recognition software could easily eliminate this issue. If weld inspectors are aware their work will be 100% machine certified and can be independently verified, this type of fraud can be minimized.

2. User Experience – Vendor software could be used to efficiently monitor the user experience and recommend improvements to the programming and 'look and feel' of the GUI.

7. Summary

New build NPP projects deserve 21st century technology for storage and retrieval of plant data. With the life cycle of an NPP stretching out to nearly 100 years, a significant effort in planning the system for the storage of such data is warranted.

Outlined here are ideas for a secure and efficient framework for such a system with key processes, criteria, and best practices identified, including:

1) User Productivity
2) Security
3) Economics
4) Disaster Recovery
5) Automation
6) AI/ML
7) Regulatory Compliance

Any program which considers the information provided here in the intial stage is considered to have a very good opportunity for success for the life of the project.

REFERENCES

[1] NARA, *Criteria for Successfully Managing Permanent Electronic Records,* National Archives and Records Administration, US Federal Government, March 16, 2018.

[2] IAEA-TECDOC-1651, *Information Technology for Nuclear Power Plant Configuration Management,* International Nuclear Energy Agency, Vienna, Austria, July 2010.

[3] IAEA-TECDOC-1555, *Managing the First Nuclear Power Plant Project,* International Nuclear Energy Agency, Vienna, Austria, May 2007.